(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
1 mai 2003 (01.05.2003)

PCT

(10) Numéro de publication internationale
WO 03/036863 A1

(51) Classification internationale des brevets[7] : H04L 9/30

(21) Numéro de la demande internationale :
PCT/FR02/03665

(22) Date de dépôt international :
24 octobre 2002 (24.10.2002)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
01/13787 25 octobre 2001 (25.10.2001) FR

(71) Déposants *(pour tous les États désignés sauf US)* : **FRANCE TELECOM** [FR/FR]; 6, place d'Alleray, F-75015 Paris (FR). **CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE** [FR/FR]; 3, rue Michel-Ange, F-75794 Paris Cedex 16 (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **GIRAULT, Marc** [FR/FR]; 4, rue Viviane, F-14000 Caen (FR). **MISARSKY, Jean-François** [FR/FR]; 126, rue de Bayeux, Escalier 5, F-14000 Caen (FR). **DEHORNOY, Patrick** [FR/FR]; 11, impasse du Vivier, F-27180 Amières Sur Iton (FR). **SIBERT, Hervé** [FR/FR]; 26bis, rue du Régiment de Maisonneuve, F-14123 Fleury Sur Orne (FR).

(74) Mandataire : **LEMOYNE, Didier**; France Telecom R & D/VAT/PI, 38-40, rue du Général Leclerc, F-92794 Issy Moulineaux Cedex 9 (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclaration en vertu de la règle 4.17 :
— *relative à la qualité d'inventeur (règle 4.17.iv)) pour US seulement*

Publiée :
— *avec rapport de recherche internationale*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(54) Title: PUBLIC KEY CRYPTOGRAPHIC METHOD BASED ON BRAID GROUPS

(54) Titre : PROCEDE CRYPTOGRAPHIQUE A CLE PUBLIQUE BASE SUR LES GROUPES DE TRESSES

(57) Abstract: The invention concerns a public key cryptographic method based on braid groups. The invention is characterized in that the method uses: a secret key, defined by a representative s selected from a given braid S in a braid group G, a public key, defined in particular by a representative v of the braid T(S), transformed from the braid S by an operator T, at least an operation verifying equality between two braids, that is equivalence of representatives of said two braids. The invention is applicable to quick execution public key cryptography.

(57) Abrégé : Procédé cryptographique à clé publique basé sur les groupes de tresses. Selon l'invention, ledit procédé met en oeuvre; une clé secrète, définie par un représentant s choisi d'une tresse donnée S dans un groupe de tresses G; une clé publique, définie notamment par un représentant v de la tresse T(S), transformée de la tresse S par un opérateur T; au moins une opération de vérification de l'égalité de deux tresses, c'est à dire de l'équivalence de représentants de ces deux tresses. Application aux procédés de cryptographie à clé publique d'exécution rapide.

WO 03/036863 A1

PROCEDE CRYPTOGRAPHIQUE A CLE PUBLIQUE BASE SUR LES GROUPES DE TRESSES

La présente invention concerne un procédé cryptographique à clé publique basé sur les groupes de tresses.

L'invention trouve une application particulièrement avantageuse dans le domaine des procédés de cryptographie à clé publique d'exécution rapide, notamment dans des environnements peu dotés de ressources, tels que les cartes à microprocesseur standards, avec ou sans contacts.

Dans le domaine de la cryptographie à clé publique, chaque utilisateur détient une paire de clés pour un usage donné, ladite paire étant constituée d'une clé secrète et d'une clé publique associée. Par exemple, s'il s'agit d'une paire de clés dédiée à la confidentialité, alors la clé publique est utilisée pour chiffrer les données, tandis que la clé secrète est utilisée pour les déchiffrer, c'est à dire pour rétablir les données en clair. Par contre, s'il s'agit d'une paire de clés dédiée à l'authentification, alors la clé secrète est utilisée pour calculer des valeurs d'authentification, tandis que la clé publique est utilisée pour vérifier ces valeurs d'authentification. D'autres usages, tels que signatures numériques ou échanges de clés, sont également possibles.

La cryptographie à clé publique est d'une très grande utilité dans la mesure où, contrairement à la cryptographie à clé secrète, elle n'exige pas que les interlocuteurs partagent le même secret pour établir une communication sécurisée. Cependant, cet avantage en terme de sécurité s'accompagne d'un désavantage en terme de performance, car les procédés de cryptographie à clé publique (encore appelés « schémas à clé publique ») sont souvent cent ou mille fois plus lents que les procédés de cryptographie dits à clé secrète (encore appelés « schémas à clé secrète »). C'est donc un défi très important que de trouver des procédés de cryptographie à clé publique d'exécution rapide, de façon à pouvoir les mettre en œuvre dans les environnements dotés de peu de ressources évoqués plus haut, comme les cartes à microprocesseur.

La plupart des schémas à clé publique existant actuellement reposent sur la difficulté de problèmes mathématiques issus du domaine de l'arithmétique, ou « théorie des nombres ». C'est ainsi que la sécurité du

schéma de chiffrement et de signature électronique connu sous le nom de RSA (du nom de ses auteurs : Rivest, Shamir et Adleman) repose sur la difficulté du problème de la factorisation des entiers : étant donné un grand nombre entier (plus de 1 000 bits) égal au produit de deux ou plusieurs facteurs premiers de tailles comparables, il n'existe pas de méthode efficace pour retrouver ces facteurs premiers.

D'autres schémas à clé publique, tels que le schéma de signature électronique décrit dans le brevet français n° 2 716 058, font reposer la sécurité sur la difficulté du problème du logarithme discret. Tous ces schémas ont en commun d'utiliser comme opérations de base des opérations sur des entiers, comme des multiplications modulaires : ab (modulo n), des divisions modulaires : a/b (modulo n), ou encore des exponentiations modulaires : a^b (modulo n) où a et b sont des entiers.

Le fait que la plupart des schémas à clé publique existants reposent sur l'arithmétique présente au moins deux inconvénients.

Le premier inconvénient est que l'existence d'algorithmes efficaces pour résoudre le problème de la factorisation et celui du logarithme discret lorsque les entiers considérés ont une longueur de quelques centaines de bits, implique de prendre des longueurs d'entiers (en particulier des longueurs de clés) très élevées, c'est à dire 1 000 bits ou plus à l'heure actuelle. Il s'ensuit des difficultés de stockage et, surtout, des temps de calcul eux-mêmes très élevés. De plus, l'efficacité de ces algorithmes s'accroissant assez rapidement avec le temps, les longueurs de clés doivent être augmentées en conséquence.

Le deuxième inconvénient est qu'il est dangereux de faire reposer la sécurité de la majorité des applications sécurisées sur la difficulté de deux problèmes mathématiques seulement. Ceci est d'autant plus vrai que ces deux problèmes sont voisins l'un de l'autre et il est tout à fait plausible que la découverte d'un algorithme efficace pour l'un s'accompagne d'un algorithme efficace de résolution pour l'autre.

C'est pourquoi, depuis une quinzaine d'années, beaucoup d'efforts ont été faits pour construire des schémas cryptographiques à clé publique qui reposent sur d'autres problèmes que les deux mentionnés ci-dessus et/ou sur d'autres objets mathématiques que des entiers. En particulier, il a été proposé de remplacer les opérations sur des entiers par des opérations sur les points

de courbes dites « elliptiques ». La motivation en est que le problème du logarithme discret semble encore plus difficile à résoudre dans les courbes elliptiques, ce qui permet de réduire les longueurs de clés sans compromettre la sécurité des schémas considérés.

Cependant, l'utilisation de courbes elliptiques ne résout que partiellement les deux problèmes soulevés ci-dessus. En effet, même si les courbes elliptiques sont des objets mathématiques différents et plus complexes que les ensembles d'entiers, elles en restent relativement proches en ce sens que la théorie qui les décrit a des relations très étroites avec la théorie des nombres. Un effet tangible de cette proximité est que les calculs à effectuer sur les courbes elliptiques se ramènent à une succession d'opérations sur des entiers semblables à celles définies plus haut, même si les entiers sont de taille inférieure. Une conséquence est que les temps de calcul restent trop élevés.

Il subsiste donc la nécessité d'utiliser à des fins cryptographiques des objets mathématiques très différents de ceux que fournissent la théorie des nombres et celles qui lui sont proches, de manière, d'une part, à disposer de solutions de remplacement en cas de découverte d'algorithmes efficaces pour résoudre les problèmes puisés dans les théories ci-dessus et, d'autre part, à disposer de solutions extrêmement efficaces en terme de performance et, notamment, en terme de temps de calcul.

Des tentatives ont été faites dans ce sens. L'une d'elles (voir K.H.Ko, S.J.Lee, J.H.Cheon, J.W.Han, J.Kang et C.Park, *New Public-Key Cryptosystem Using Braid Groups*, Advances in Cryptology, LNCS 1880, p.166-183, Springer Verlag, août 2000) consiste à utiliser des objets mathématiques appelés « groupes de tresses ».

Une tresse, au sens mathématique du terme, est une conceptualisation et une généralisation de la notion de tresse au sens géométrique et ordinaire du terme. Pour plus de détails sur la théorie des tresses, on se reportera à l'article de P.Dehornoy, *L'art de tresser*, Pour la Science, Dossier hors-série « La science des nœuds », p.68-75, 1997.

L'ensemble des « tresses à n brins » constitue un groupe **G**, muni d'une loi de composition interne appelée produit qui, à deux tresses X et Y, associe une tresse notée XY, résultat de l'opération consistant à « attacher » la tresse Y sous la tresse X. En général, le produit de tresses n'est pas une

opération commutative. De plus, à toute tresse à n brins on peut associer de manière unique une permutation de l'ensemble {1,2,...,n}. Une tresse dont la permutation est la permutation identité (qui envoie tout entier de 1 à n sur lui-même) est dite pure.

Le groupe **G** de tresses à n brins est doté d'un élément neutre E, représenté par n brins non tressés, tel que, pour toute tresse X, les produits EX et XE sont tous deux égaux à X. De plus, toute tresse X possède un inverse noté X^{-1} tel que les produits XX^{-1} et $X^{-1}X$ sont tous deux égaux à E.

Les tresses à n brins du groupe **G** peuvent être codées de plusieurs manières, appelées représentations. Pour coder une tresse dans une représentation donnée, on lui associe un ou plusieurs « représentants ». Si X est une tresse, on notera x un représentant de X dans la représentation sous-jacente. Dans les représentations usuelles telles que celles utilisées par la présente invention, si une tresse X et une tresse Y ont respectivement comme représentants x et y, alors il existe une opération simple sur x et y dont le résultat, noté xy, est un représentant de la tresse XY, de même qu'il existe une opération simple sur x dont le résultat, noté x^{-1}, est un représentant de la tresse X^{-1}.

La représentation la plus répandue, dite « standard », repose sur le fait que toute tresse peut se décomposer comme un produit de n-1 tresses élémentaires, que l'on note chacune par une lettre d'un alphabet, et de leurs inverses. On notera par des lettres minuscules des représentants de ces tresses élémentaires. Par exemple, dans le cas des tresses à 4 brins, on note les 3 tresses élémentaires A, B, et C, de sorte qu'une tresse quelconque X du groupe peut s'exprimer en fonction des tresses A, B, C, et de leurs inverses A^{-1}, B^{-1}, C^{-1}, et ceci de manière non unique. Par exemple, les tresses ABA et BAB sont égales. On dira que aba et bab sont des représentants de tresse équivalents, c'est-à-dire qu'ils représentent la même tresse. De même, la tresse B est égale à la tresse BBB^{-1}, de sorte que les représentants b et bbb^{-1} sont équivalents.

D'autres représentations, que l'on dira « alternatives », du groupe **G** peuvent être employées. Ainsi, une tresse à n brins peut être codée comme un produit de tresses « simples » ou « canoniques », représentées par des permutations de {1,2,...,n}, et de leurs inverses. Mentionnons encore une représentation de **G** appelée « représentation de Birman-Ko-Lee », où le

codage se fait encore à l'aide de permutations, ou à l'aide de certains tableaux de n nombres tous compris entre 1 et n, et une autre, appelée représentation de Dynnikov, où le codage se fait à l'aide d'entiers. Là encore, une tresse peut avoir plusieurs représentants, et des représentants d'une même tresse sont dits équivalents.

Dans la représentation dite « standard », où une tresse est codée par des mots, on introduit la notation « ~ », signifiant « équivalent à ». On notera « u~v », où u est un représentant de la tresse U, et v un représentant de la tresse V, lorsque les tresses U et V sont égales. Les relations d'équivalence suivantes permettent exactement de déterminer si deux mots représentent la même tresse :

- aa^{-1}~$a^{-1}a$~e,
- ac~ca si a et c sont des lettres non consécutives,
- aba~bab si a et b sont des lettres consécutives.

Le procédé de cryptographie à clé publique utilisant les tresses précédemment cité est exclusivement dédié à la confidentialité des données, qui sont chiffrées avant d'être transmises, puis déchiffrées par le destinataire.

Le problème technique à résoudre par l'objet de la présente invention est de proposer un procédé de cryptographie à clé publique basé sur les groupes de tresses, qui, d'une part, permettrait non seulement d'assurer la confidentialité des données mais aussi l'authentification d'entités et/ou de données et, d'autre part, permettrait d'obtenir, à la fois, un niveau de sécurité élevé et des temps de calcul rapides, compatibles avec une application du procédé à des systèmes à ressources limitées en puissance, comme les cartes à microprocesseurs.

La solution au problème technique posé consiste, selon la présente invention, en ce que ledit procédé met en œuvre :

- une clé secrète, définie par un représentant s d'une tresse donnée S dans un groupe de tresses **G**,
- une clé publique, définie notamment par un représentant v d'une tresse T(S), transformée de la tresse S par un opérateur T,
- au moins une opération de vérification de l'égalité de deux tresses, c'est-à-dire de l'équivalence de représentants de ces deux tresses.

Ainsi, on comprend que la sécurité du procédé cryptographique selon l'invention repose sur la difficulté de reconstituer la tresse secrète S à partir

du représentant v de T(S) contenu dans la clé publique, cette reconstitution se heurtant cumulativement au problème de l'égalité de tresses, donc de l'équivalence de représentants, et à celui de l'inversion de l'opérateur T. En ce sens, il est proposé deux exemples pour l'opérateur T pouvant convenir à la mise en œuvre du procédé, objet de l'invention :

- l'opérateur T est défini par $T(S)=SWS^{-1}$, où W est une tresse d'un groupe **G** dont un représentant w forme, avec un représentant v de $V=T(S)$, ladite clé publique, et S^{-1} la tresse inverse de S dans le groupe **G**,
- l'opérateur T est défini par la donnée d'un entier positif p au moins égal à 2, et par $T(S)=S^p=S...S$, produit de S p fois.

Le premier opérateur met en jeu le problème de la conjugaison, considéré comme extrêmement difficile : il s'agit, connaissant un représentant de la tresse SWS^{-1}, de trouver un représentant de la tresse S. En particulier, l'utilisation de formes réduites, qui sont des représentants privilégiés des tresses, rend ce problème particulièrement inextricable. Il en est de même du problème de la racine, mis en œuvre dans le deuxième opérateur : trouver un représentant de S connaissant un représentant de S^p est, en pratique, une opération irréalisable.

Par ailleurs, l'opération de vérification d'équivalence de représentants de tresses est rendue d'autant plus rapide, qu'elle est réalisée au moyen d'une forme réduite des représentants desdites tresses, ou de la forme réduite de représentants de tresses calculées à partir desdites tresses. L'intérêt de ces formes réduites, fonctions qui transforment un représentant d'une tresse en un autre représentant (éventuellement identique) de cette même tresse, est qu'elles fournissent en effet des méthodes efficaces pour résoudre le problème, non trivial a priori, de savoir si deux tresses sont égales, à partir de représentants desdites tresses.

Une forme réduite FR est caractérisée par le fait qu'elle transforme tout représentant de la tresse neutre E en un représentant trivial (c'est-à-dire vide) noté e. Cependant, deux représentants d'une même tresse n'ont pas forcément la même forme réduite. Il en est ainsi de la forme réduite développée par P.Dehornoy, *A Fast Method for Comparing Braids*, Advances in Mathematics, n°125, pp.200-235,1997. Pour savoir si deux représentants u et v de tresses U et V sont équivalents, on calcule la forme réduite de uv^{-1}, qui

est un représentant de la tresse UV^{-1}. En effet, il revient au même de dire que u et v sont équivalents, ou que uv^{-1} représente la tresse triviale E. Ainsi, u et v sont équivalents, si et seulement si $FR(uv^{-1})=e$. De façon alternative, on peut utiliser $u^{-1}v$ au lieu de uv^{-1}.

Un cas particulier de formes réduites est constitué par les formes normales. Une forme normale FN est une forme réduite qui, à deux représentants quelconques d'une même tresse, associe le même représentant de cette tresse. En d'autres termes, deux représentants u et v de tresses sont équivalents, si et seulement si ils ont la même forme normale FN(u)=FN(v). Plusieurs façons de définir une telle forme normale FN sont décrites dans l'état de la technique, en particulier dans D. Epstein et al., *Word Processing in Groups*, Jones and Barlett Publishers, Boston, 1988. Certaines formes normales peuvent être calculées de manière efficace, en particulier dans le cas des représentations « alternatives » du groupe de tresses décrites précédemment : les représentants des tresses se prêtent alors particulièrement au calcul de formes normales.

Cependant, dans le cas de la représentation « standard », l'utilisation d'une forme réduite permet d'obtenir des algorithmes plus efficaces, ceci étant dû au fait que les exigences sur une forme réduite sont moins fortes que sur une forme normale, deux représentants équivalents n'ayant pas nécessairement même forme réduite, alors qu'ils ont nécessairement la même forme normale. C'est ainsi que l'algorithme calculant une forme réduite cité ci-dessus, est plus rapide que tout algorithme connu calculant une forme normale dans le cas de la représentation « standard ». On comprend alors que, suivant le choix de la représentation, il y aura avantage à mettre en œuvre le procédé cryptographique de l'invention tantôt avec une forme réduite non nécessairement normale notée FR (typiquement, en représentation « standard »), tantôt avec une forme réduite normale notée FN (en particulier dans les représentations « alternatives »).

On notera que le fait qu'une forme réduite ne soit éventuellement pas unique pour une tresse donnée ne constitue pas un inconvénient lorsqu'une décision à prendre dépend seulement du fait que deux mots soient équivalents ou non ; par exemple « L'entité avec laquelle on communique est-elle authentique ou non ? ».

Quatre exemples d'application du procédé cryptographique conforme à l'invention vont maintenant être décrits en détail qui, de manière non limitative, sont tous des protocoles d'authentification.

De même, et bien que cela ne soit pas indispensable, comme on l'a vu plus haut, on utilisera systématiquement des formes réduites FR, qui ne sont pas nécessairement des formes normales, sachant qu'elles constituent le mode de réalisation préféré de l'invention.

Le premier protocole d'authentification fait intervenir un groupe **G1** de tresses à n=p+q brins et le problème de la conjugaison. Plus précisément, deux tresses d'un type particulier sont impliquées : l'une n'utilise que les p brins de gauche, et peut être codée, dans la représentation « standard », à l'aide des p-1 premières lettres et de leurs inverses dans un alphabet à n=p+q lettres, l'autre n'utilise que les q brins de droite, et par conséquent peut être codée, dans la représentation « standard », à l'aide des q-1 dernières lettres de cet alphabet et de leurs inverses. Deux telles tresses présentent la caractéristique de commuter l'une avec l'autre, contrairement au cas général.

La clé secrète du prouveur A est un représentant s d'une tresse S à p brins de gauche. La clé publique du prouveur A, utilisée par le vérificateur B, est une paire (v,w), constituée par un représentant w d'une tresse W choisie dans le groupe **G1**, et par un représentant v de la tresse $V=T(S)=SWS^{-1}$.

L'authentification du prouveur A par le vérificateur B se déroule de la manière suivante, en deux échanges :

1. B choisit une tresse Z à q brins de droite, par choix d'un représentant z. B détient alors un représentant, noté zwz^{-1}, de la tresse $C=ZWZ^{-1}$. B calcule un représentant $c=F1(zwz^{-1})$ de C, et envoie c à A.
2. A calcule un représentant $y=F2(scs^{-1})$ de la tresse SCS^{-1}, et envoie y à B. B vérifie l'équivalence $y\sim zvz^{-1}$, par utilisation d'une forme réduite FR (éventuellement normale).

Le fait que y est équivalent à zvz^{-1} provient de ce que S et Z commutent l'une avec l'autre ; en effet, y représente la tresse SCS^{-1} c'est-à-dire :

$S(ZWZ^{-1})S^{-1}=(SZ)W(Z^{-1}S^{-1})=(ZS)W(S^{-1}Z^{-1})=Z(SWS^{-1})Z^{-1}=ZVZ^{-1}$, qui est aussi représentée par zvz^{-1}.

La vérification de l'équivalence formulée dans l'étape 2 peut se faire, de manière non exclusive, par la vérification de l'égalité $FR(yzv^{-1}z^{-1})=e$, ou, si l'on utilise une forme normale, $FN(y)=FN(zvz^{-1})$.

Les fonctions F1 et F2 sont des fonctions qui, à un représentant d'une tresse, associent un représentant de cette même tresse. Dans le cas de la représentation « standard », F1 et F2 pourront être, mais pas nécessairement, des formes réduites. Elles seront, typiquement, des formes réduites, généralement autres que celle utilisée pour la vérification d'équivalence. Dans le cas de représentations alternatives, on prendra pour F1 et F2 la forme normale FN.

Par ailleurs, on choisira préférentiellement pour W une tresse pure.

Des variantes de ce protocole peuvent être facilement spécifiées. En particulier, on peut choisir pour v un représentant de la tresse $T'(S)=S^{-1}WS$ et modifier le reste du protocole en conséquence. Ou encore, on peut choisir pour S une tresse sur les q brins de droite, et pour Z une tresse sur les p brins de gauche.

Le deuxième protocole d'authentification fait intervenir un groupe **G2** de tresses à n brins et le problème de la conjugaison. Il consiste à itérer k fois un protocole de base à 3 échanges, ce dernier n'offrant à lui seul qu'une chance sur deux de détecter un éventuel imposteur, à savoir une entité C, ignorant le secret de A, mais essayant de se faire passer pour A. A l'issue des k itérations, un imposteur n'a plus qu'une chance sur 2^k de ne pas être détecté. Ce protocole relève de la catégorie des protocoles à connaissance nulle (« zero-knowledge »).

La clé secrète du prouveur A est un représentant s d'une tresse S du groupe **G2**. La clé publique du prouveur A, utilisée par le vérificateur B, est une paire (v,w), constituée par un représentant w d'une tresse W choisie dans le groupe **G2**, et par un représentant v de la tresse $V=T(S)=SWS^{-1}$.

L'authentification du prouveur A par le vérificateur B se déroule de la manière suivante, en trois échanges itérés k fois :

1. A choisit une tresse R, par choix d'un représentant r. A détient donc un représentant rwr^{-1} de la tresse $X=RWR^{-1}$. A calcule un représentant $x=F1(rwr^{-1})$ de X, et envoie x à B,
2. B tire au hasard un bit c et envoie c à A,

3a. Si c=0, A pose y=r et envoie y à B. B vérifie l'équivalence $x \sim ywy^{-1}$, par utilisation d'une forme réduite FR (éventuellement normale).

3b. Si c=1, A calcule un représentant $y=F2(rs^{-1})$ de la tresse RS^{-1}, et envoie y à B. B vérifie alors l'équivalence $x \sim yvy^{-1}$, par utilisation d'une forme réduite FR (éventuellement normale).

En effet, lorsque c=1, x et yvy^{-1} sont équivalents puisque yvy^{-1} représente la tresse $(RS^{-1})SWS^{-1}(SR^{-1})=R(S^{-1}S)W(S^{-1}S)R^{-1}=RWR^{-1}$, dont x est un représentant.

La vérification de l'équivalence formulée dans l'étape 3a peut se faire, de manière non exclusive, par la vérification de l'égalité $FR(xyw^{-1}y^{-1})=e$, ou, si l'on utilise une forme normale, $FN(x)=FN(ywy^{-1})$.

La vérification de l'équivalence formulée dans l'étape 3b peut se faire, de manière non exclusive, par la vérification de l'égalité $FR(xyv^{-1}y^{-1})=e$, ou, si l'on utilise une forme normale, $FN(x)=FN(yvy^{-1})$.

Les fonctions F1 et F2 sont des fonctions qui, à un représentant d'une tresse, associent un représentant de cette même tresse. Dans le cas de la représentation « standard », F1 et F2 pourront être, mais pas nécessairement, des formes réduites. Elles seront, typiquement, des formes réduites, généralement autres que celle utilisée pour la vérification d'équivalence. Dans le cas de représentations alternatives, on prendra de préférence pour F1 et F2 la forme normale FN.

Des variantes de ce protocole peuvent être facilement spécifiées. En particulier, on peut choisir pour v un représentant de la tresse $T'(S)=S^{-1}WS$ et modifier le reste du protocole en conséquence.

Le troisième protocole d'authentification fait intervenir un groupe **G**3 de tresses à n brins et le problème de la conjugaison. Comme le précédent, ce protocole relève de la catégorie des protocoles à connaissance nulle, trois échanges étant itérés k fois.

La clé secrète du prouveur A est un représentant s d'une tresse S du groupe **G**3. La clé publique du prouveur A, utilisée par le vérificateur B, est une paire (v,w), constituée par un représentant w d'une tresse W choisie dans le groupe **G**3, et par un représentant v de la tresse $V=T(S)=SWS^{-1}$.

L'authentification du prouveur A par le vérificateur B se déroule de la manière suivante, en trois échanges itérés k fois :

1. A choisit une tresse R, par choix d'un représentant r. A détient donc un représentant rwr^{-1} de la tresse $X=RWR^{-1}$, ainsi qu'un représentant rvr^{-1} de la tresse $X'=RVR^{-1}$. A calcule un représentant $x=F1(rwr^{-1})$ de X, un représentant $x'=F'1(rvr^{-1})$ de X', et envoie x et x' à B,
2. B tire au hasard un bit c et envoie c à A,

3a. Si c=0, A pose y=r et envoie y à B. B vérifie les équivalences $x\sim ywy^{-1}$ et $x'\sim yvy^{-1}$, par utilisation d'une forme réduite FR (éventuellement normale).

3b. Si c=1, A calcule un représentant $y=F2(rsr^{-1})$ de la tresse RSR^{-1}, et envoie y à B. B vérifie alors l'équivalence $x'\sim yxy^{-1}$, par utilisation d'une forme réduite FR (éventuellement normale).

En effet, lorsque c=1, x' et yxy^{-1} sont équivalents puisque yxy^{-1} représente la tresse :
$(RSR^{-1})RWR^{-1}(RS^{-1}R^{-1})=RS(R^{-1}R)W(R^{-1}R)S^{-1}R^{-1}=R(SWS^{-1})R^{-1}=RVR^{-1}$, dont x' est un représentant.

La vérification de l'équivalence formulée dans l'étape 3a peut se faire, de manière non exclusive, par la vérification des égalités $FR(xyw^{-1}y^{-1})=e$ et $FR(x'yv^{-1}y^{-1})=e$, ou, si l'on utilise une forme normale, $FN(x)=FN(ywy^{-1})$ et $FN(x)=FN(yvy^{-1})$.

La vérification de l'équivalence formulée dans l'étape 3b peut se faire, de manière non exclusive, par la vérification de l'égalité $FR(x'yx^{-1}y^{-1})=e$, ou, si l'on utilise une forme normale, $FN(x')=FN(yxy^{-1})$.

Les fonctions F1, F'1 et F2 sont des fonctions qui, à un représentant d'une tresse, associent un représentant de cette même tresse. Dans le cas de la représentation « standard », F1, F'1 et F2 pourront être, mais pas nécessairement, des formes réduites. Elles seront, typiquement, des formes réduites, généralement autres que celle utilisée pour la vérification d'équivalence. Dans le cas de représentations alternatives, on prendra de préférence pour F1 et F'1, et F2 la forme normale FN.

On remarquera que la propriété utilisée dans la vérification est le fait que la conjugaison est auto-distributive. On rappelle qu'une opération * est dite auto-distributive si l'on a : $u*(v*w)=(u*v)*(u*w)$. Ainsi, l'opération de conjugaison pourrait-elle être remplacée dans ce protocole par une autre opération auto-distributive.

Le quatrième protocole d'authentification fait intervenir un groupe **G4** de tresses à n brins et, simultanément, le problème de la racine p-ième et le problème de la conjugaison. Ce protocole relève de la catégorie des protocoles à connaissance nulle au sens des deux précédents.

La clé secrète du prouveur A est un représentant s d'une tresse S du groupe **G4**. La clé publique du prouveur A, utilisée par le vérificateur B, est un représentant v de la tresse $V= S^p =S...S$, produit de S itéré p fois, avec p un petit entier supérieur ou égal à 2.

L'authentification du prouveur A par le vérificateur B se déroule de la manière suivante, en trois échanges itérés k fois :

1. A choisit une tresse R, par choix d'un représentant r. A détient donc un représentant rvr^{-1} de la tresse $X=RVR^{-1}$. A calcule un représentant $x=F1(rvr^{-1})$ de X, et envoie x à B,
2. B tire au hasard un bit c et envoie c à A,

3a. Si c=0, A pose y=r et envoie y à B. B vérifie l'équivalence $x\sim yvy^{-1}$, par utilisation d'une forme réduite FR (éventuellement normale).

3b. Si c=1, A calcule un représentant $y=F2(rsr^{-1})$ de la tresse RSR^{-1}, et envoie y à B. B vérifie alors l'équivalence $x\sim y^p$, par utilisation d'une forme réduite FR (éventuellement normale).

En effet, lorsque c=1, x et y^p sont équivalents puisque y^p représente la tresse $(RSR^{-1})^p=RS^pR^{-1}=RVR^{-1}$, dont x est un représentant.

La vérification de l'équivalence formulée dans l'étape 3a peut se faire, de manière non exclusive, par la vérification de l'égalité $FR(xyv^{-1}y^{-1})=e$, ou, si l'on utilise une forme normale, $FN(x)=FN(yvy^{-1})$.

La vérification de l'équivalence formulée dans l'étape 3b peut se faire, de manière non exclusive, par la vérification de l'égalité $FR(vy^{-1}...y^{-1})=e$ (y^{-1} étant itéré p fois), ou, si l'on utilise une forme normale, FN(v)=FN(y...y) (y étant itéré p fois).

Les fonctions F1 et F2 sont des fonctions qui, à un représentant d'une tresse, associent un représentant de cette même tresse. Dans le cas de la représentation « standard », F1 et F2 pourront être, mais pas nécessairement, des formes réduites. Elles seront, typiquement, des formes réduites, généralement autres que celles utilisées pour la vérification d'équivalence. Dans le cas de représentations alternatives, on prendra de préférence pour F1 et F2 la forme normale FN.

REVENDICATIONS

1. Procédé cryptographique à clé publique basé sur les groupes de tresses, caractérisé en ce que ledit procédé met en œuvre :
   - une clé secrète, définie par un représentant s d'une tresse donnée S dans un groupe de tresses **G**,
   - une clé publique, définie notamment par un représentant v de la tresse T(S), transformée de la tresse S par un opérateur T,
   - au moins une opération de vérification de l'égalité de deux tresses, c'est à dire de l'équivalence de représentants de ces deux tresses.
2. Procédé cryptographique selon la revendication 1, caractérisé en ce que le représentant v est la forme réduite FR d'un représentant de la tresse T(S).
3. Procédé cryptographique selon l'une des revendications 1 ou 2, caractérisé en ce que ladite opération de vérification de l'équivalence de représentants de deux tresses est réalisée au moyen de la forme réduite FR de représentants de ces deux tresses, ou de la forme réduite de représentants de tresses calculées à partir desdites tresses.
4. Procédé cryptographique selon l'une des revendications 2 ou 3, caractérisé en ce que ladite forme réduite FR est une forme normale FN.
5. Procédé cryptographique selon l'une des revendications 2 ou 3, caractérisé en ce que ladite forme réduite FR est une forme réduite non normale.
6. Procédé cryptographique selon l'une quelconque des revendications 1 à 5, caractérisé en ce que l'opérateur T est défini par $T(S)=SWS^{-1}$, où W est une tresse d'un groupe **G**, et dont un représentant w forme, avec le représentant v de la tresse V, ladite clé publique, et S^{-1} la tresse inverse de la tresse S dans le groupe **G**.
7. Procédé cryptographique selon l'une quelconque des revendications 1 à 5, caractérisé en ce que l'opérateur T est défini par la donnée d'un entier positif p au moins égal à 2, et par $T(S)=S^p=S...S$, produit de S p fois.

8. Procédé cryptographique selon la revendication 6, caractérisé en ce que, pour effectuer une authentification d'un prouveur A par un vérificateur B :
   - on attribue au prouveur A une clé secrète constituée par un représentant s d'une tresse S à p brins de gauche choisie dans un groupe **G1** de tresses à n=p+q brins,
   - on attribue au prouveur A une clé publique, utilisée par le vérificateur B, constituée d'un représentant w d'une tresse W choisie dans le groupe **G1** et d'un représentant v de la tresse $V=T(S)=SWS^{-1}$,
   - le vérificateur B choisit dans le groupe **G1** une tresse Z à q brins de droite, par choix d'un représentant z, calcule un représentant c de la tresse $C=ZWZ^{-1}$, et envoie c au prouveur A,
   - le prouveur A calcule un représentant y de la tresse $Y=SCS^{-1}$ et envoie y au vérificateur B,
   - le vérificateur B vérifie l'équivalence des représentants y et zvz^{-1}.

9. Procédé cryptographique selon la revendication 6, caractérisé en ce que, pour effectuer une authentification d'un prouveur A par un vérificateur B :
   - on attribue au prouveur A une clé secrète constituée par un représentant s d'une tresse S choisie dans un groupe **G2** de tresses à n brins,
   - on attribue au prouveur A une clé publique, utilisée par le vérificateur B, constituée d'un représentant w d'une tresse W choisie dans le groupe **G2** et d'un représentant v de la tresse SWS^{-1},
   - le prouveur A choisit une tresse R dans le groupe **G2**, par choix d'un représentant r, calcule un représentant x de la tresse $X=RWR^{-1}$, et envoie x au vérificateur B,
   - le vérificateur B choisit un bit c et envoie c au prouveur A,
     - si c=0, le prouveur A pose y=r et envoie y au vérificateur B qui vérifie l'équivalence des représentants x et ywy^{-1},
     - si c=1, le prouveur A calcule un représentant y de la tresse RS^{-1} et envoie y au vérificateur B, qui vérifie l'équivalence des représentants x et yvy^{-1},

les trois derniers échanges étant itérés k fois.

10. Procédé cryptographique selon la revendication 6, caractérisé en ce que, pour effectuer une authentification d'un prouveur A par un vérificateur B :

- on attribue au prouveur A une clé secrète constituée par un représentant s d'une tresse S choisie dans un groupe **G3** de tresses à n brins,
- on attribue au prouveur A une clé publique, utilisée par le vérificateur B, constituée d'un représentant w d'une tresse W choisie dans le groupe **G3** et d'un représentant v de la tresse SWS^{-1},
- le prouveur A choisit une tresse R dans le groupe **G3**, par choix d'un représentant r, calcule un représentant x de la tresse $X=RWR^{-1}$, un représentant x' de la tresse $X'=RVR^{-1}$, et envoie x et x' au vérificateur B,
- le vérificateur B choisit un bit c et envoie c au prouveur A,
    - si c=0, le prouveur A pose y=r et envoie y au vérificateur B qui vérifie l'équivalence des représentants x et ywy^{-1} et celle des représentants x' et yvy^{-1},
    - si c=1, le prouveur A calcule un représentant y de la tresse RSR^{-1} et envoie y au vérificateur B, qui vérifie l'équivalence des représentants x' et yxy^{-1},

les trois derniers échanges étant itérés k fois.

11. Procédé cryptographique selon la revendication 7, caractérisé en ce que, pour effectuer une authentification d'un prouveur A par un vérificateur B :

- on attribue au prouveur A une clé secrète constituée par un représentant s d'une tresse S choisie dans un groupe **G4** de tresses à n brins,
- on attribue au prouveur A une clé publique, utilisée par le vérificateur B, constituée par un représentant v de la tresse $V=S^p=S...S$, produit de S p fois, p étant un entier supérieur ou égal à 2,

- le prouveur A choisit une tresse R dans le groupe G3, par choix d'un représentant r, calcule un représentant x de la tresse $X=RVR^{-1}$, et envoie x au vérificateur B,
- le vérificateur B choisit un bit c et envoie c au prouveur A,
  - si c=0, le prouveur A pose y=r et envoie y au vérificateur B qui vérifie l'équivalence des représentants x et yvy^{-1},
  - si c=1, le prouveur A calcule un représentant y de la tresse RSR^{-1} et envoie y au vérificateur B, qui vérifie l'équivalence des représentants x et $y^p=y...y$, représentant de la tresse Y^p obtenu à partir de y,

les trois derniers échanges étant itérés k fois.

12. Procédé cryptographique selon la revendication 6, caractérisé en ce que l'opérateur T est remplacé par une opération auto-distributive.
13. Procédé cryptographique selon la revendication 8, caractérisé en ce que ladite tresse W est pure.

INTERNATIONAL SEARCH REPORT

Internati pplication No
PCT/rR 02/03665

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
INSPEC, EPO-Internal, WPI Data, PAJ, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	ANSHEL I ET AL: "AN ALGEBRAIC METHOD FOR PUBLIC KEY CRYPTOGRAPHY" MATHEMATICAL RESEARCH LETTERS, 'Online! vol. 6, 1999, pages 1-5, XP002208338 Retrieved from the Internet: <URL:http://www-cs.engr.ccny.cuny.edu/{csm ma/MRLpap.pdf> 'retrieved on 2002-08-01! page 1, line 23 -page 2, line 23 page 3, line 15 - line 16 page 4, line 9 - line 21 --- -/--	1-3,6,7

[X] Further documents are listed in the continuation of box C.

[ ] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 January 2003	03/02/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Liebhardt, I

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Internat xplication No
PCT/FR 02/03665

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	ANSHEL I ET AL: "New key agreement protocols in braid group cryptography" , TOPICS IN CRYPTOLOGY - CT-RSA 2001. THE CRYPTOGRAPHERS' TRACK AT RSA CONFERENCE 2001. PROCEEDINGS (LECTURE NOTES IN COMPUTER SCIENCE VOL.2020), TOPICS IN CRYPTOLOGY - CT-RSA 20001, SAN FRANCISCO, CA, USA, 8-12 APRIL 2001 , 2001, BERLIN, GERMANY, SPRINGER-VERLAG, GERMANY, PAGE(S) 13 - 27 XP002208339 ISBN: 3-540-41898-9 page 18, line 21 -page 20, line 3 page 22, line 11 -page 23, line 5	2,3
A	KI HYOUNG KO ET AL: "NEW PUBLIC-KEY CRYPTOSYSTEM USING BRAID GROUPS" , ADVANCES IN CRYPTOLOGY. CRYPTO 2000. 20TH ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE, SANTA BARBARA, CA, AUG. 20 - 24, 2000. PROCEEDINGS, LECTURE NOTES IN COMPUTER SCIENCE;VOL. 1880, BERLIN: SPRINGER, DE, PAGE(S) 166-183 XP001003403 ISBN: 3-540-67907-3 cited in the application page 170, line 13 -page 171, line 14 page 173, line 14 -page 174, line 13 page 174, line 33 -page 177, line 36	1-3,6,7

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 02/03665

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/30

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
INSPEC, EPO-Internal, WPI Data, PAJ, IBM-TDB

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	ANSHEL I ET AL: "AN ALGEBRAIC METHOD FOR PUBLIC KEY CRYPTOGRAPHY" MATHEMATICAL RESEARCH LETTERS, 'en ligne! vol. 6, 1999, pages 1-5, XP002208338 Extrait de l'Internet: <URL:http://www-cs.engr.ccny.cuny.edu/{csm ma/MRLpap.pdf> 'extrait le 2002-08-01! page 1, ligne 23 -page 2, ligne 23 page 3, ligne 15 - ligne 16 page 4, ligne 9 - ligne 21 -/--	1-3,6,7

[X] Voir la suite du cadre C pour la fin de la liste des documents

[ ] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
24 janvier 2003	03/02/2003

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Liebhardt, I

RAPPORT DE RECHERCHE INTERNATIONALE

Demande nationale No
PCT/FR 02/03665

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	ANSHEL I ET AL: "New key agreement protocols in braid group cryptography" , TOPICS IN CRYPTOLOGY - CT-RSA 2001. THE CRYPTOGRAPHERS' TRACK AT RSA CONFERENCE 2001. PROCEEDINGS (LECTURE NOTES IN COMPUTER SCIENCE VOL.2020), TOPICS IN CRYPTOLOGY - CT-RSA 20001, SAN FRANCISCO, CA, USA, 8-12 APRIL 2001 , 2001, BERLIN, GERMANY, SPRINGER-VERLAG, GERMANY, PAGE(S) 13 - 27 XP002208339 ISBN: 3-540-41898-9 page 18, ligne 21 -page 20, ligne 3 page 22, ligne 11 -page 23, ligne 5	2,3
A	KI HYOUNG KO ET AL: "NEW PUBLIC-KEY CRYPTOSYSTEM USING BRAID GROUPS" , ADVANCES IN CRYPTOLOGY. CRYPTO 2000. 20TH ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE, SANTA BARBARA, CA, AUG. 20 - 24, 2000. PROCEEDINGS, LECTURE NOTES IN COMPUTER SCIENCE;VOL. 1880, BERLIN: SPRINGER, DE, PAGE(S) 166-183 XP001003403 ISBN: 3-540-67907-3 cité dans la demande page 170, ligne 13 -page 171, ligne 14 page 173, ligne 14 -page 174, ligne 13 page 174, ligne 33 -page 177, ligne 36	1-3,6,7